**Segurança**

| [Title](http://camadas.html/) | [Author](http://camadas.html/) | [Hits](http://camadas.html/) |
| --- | --- | --- |
| [Sistema Operacional](http://camadas/5-sistema-operacional.html) |  | **Hits: 0** |
| [Desktop do Administrador](http://camadas/4-desktop-do-administrador.html) |  | **Hits: 0** |
| [Servidores](http://camadas/3-servidores.html) |  | **Hits: 0** |
| [Pessoal](http://camadas/2-pessoal.html) |  | **Hits: 0** |
| [Infraestrutura](http://camadas/1-infraestrutura.html) |  | **Hits: 0** |

### **Sistema Operacional**

Atualização  
  
Importante configurar atualizações automáticas pelo menos dos pacotes de segurança  
  
**fstab**  
Criar partição para o /tmp e adicionar ao fstab  
  
sudo nano /etc/fstab  
  
/dev/sda6 /tmp ext4 defaults,nosuid,nodev,noexec 0 0  
  
**Usuário comum**  
  
Criar usuário comum e add ao sudo  
  
adduser <username>  
usermod -a -G sudo <username>  
  
**Criar chave SSH**  
Enviar para o servidor  
Acessar via SSH sem senha, com a chave  
Melhorar a segurança do SSH  
Não permita login do root ao servidor  
Limitar número de tentativas de login ao SSH  
  
MaxAuthTries 3  
  
Isso significa que após 3 tentativas incorretas de senha, a sessão será encerrada. Isso é útil, especialmente quando você deseja bloquear scripts / programas robóticos que tentam obter acesso ao seu sistema.

**Firewall**  
  
Habilitar um firewall para bloquear todas as portas, exceto as necessárias  
Sobre firewall  
  
**Desativando ICMP - não obrigatório**  
  
Muitos administradores geralmente desabilitam ou filtram as solicitações ICMP, embora isso não traga benefícios de segurança. No caso de algo como DNS, as solicitações ICMP são realmente usadas na especificação DNS para consultar se um servidor está disponível antes de enviar a solicitação DNS. As respostas ICMP também são extremamente benéficas para os servidores da web e podem servir na solução de problemas de um servidor da web que parece não estar respondendo às solicitações HTTP. A ameaça de uma inundação de ping é mínima hoje. A menos que o invasor tenha largura de banda de rede consideravelmente maior do que o alvo, a tentativa de inundação causará pouco efeito. As respostas de eco de ping consomem muito pouca CPU do alvo para responder, então é talvez um pouco como jogar muitas pedras pequenas na tentativa de derrubar uma parede de tijolos. É por isso que a maioria dos ataques DoS hoje se concentra em solicitações HTTP em vez de ICMP para aumentar o uso da CPU e da memória do servidor web, que é muito mais eficaz de executar. Resumindo, não há razão para desabilitar o ICMP.

### **Desktop do administrador**

- Uma boa máquina, rápida, estável, com um bom espaço em disco  
 - Idealmente seu sistema oepracional é uma cópia do servidos: SO, distro, versão, serviços e configurações. Caso monitore mais de um servidor talvez deva ter uma cópia de cada em uma VM ou em um containers docker ou de outra forma. Para que não fique lidando com conflitos de sistema, versão, etc.  
 - De rpeferência com vários monitores grandes para monitorar os servidores com conforto  
 - Todos os softwares de que necessida

### **Servidores**

- Sistemas operacionais  
 - Firewalls  
 - Softwares para reforçar a segurança em geral  
 - Softwares de virtualização  
 - Softwares de backup  
 - Softwares para monitoração local e remota (somente alguns)

Ok, é suficiente, pois a ideia nem é mostrar todos os detalhes de um servidor, nem mesmo muita coisa, mas apenas alertar para o fato que existem muitos pontos e cada um deles pode ser motivo de dor de cabeça. Cada detalhe precisa de atenção para que possamos dizer que nossa corrente tem a força do elo mais forte, que é idẽntica a de todos os elos. Me parece que isso é o ideal. Alias, acredito que tudo que façamos na vida deveria ser assim, ou seja, deveriamos fazer tudo bem feito, tanto porque é o melhor a fazer quanto assim estaremos mandando uma mensagem ao nosso subconsciente para que fique atento e passe a automatizar isso. Então com algum tempo estaremos dando uma forte aenção a tudo que fazemos sem esforço, de forma automática, pois o subconsciente está cuidando.  
  
  
A segurança é influenciada pela popularidade e pela facilidade de uso  
  
Quanto mais popular relativamente menos seguro  
Quanto mais amigável provavelmente menos seguro  
  
Sabe qual o tipo de hospedagem que dá o melhor desempenho de todas e também a maior segurança? A hospedagem para sites estáticos. Nada de servidor de bancos de dados nem de linguagens dinâmicas, somente o servidor web e arquivos praticamente texto, exceto o Javascript.  
Então se sua landing page for dinâmica converte em HTML estático e hospeda num Github, por exemplo e o melhor ficou para o final, é de graça. O que quer mais? Interatividade? Comentários, busca, etc. Tem como fazer. Basta procurar recursos para sites estáticos: disqus, busca do Google, etc.

### **Pessoal (que precisa de acesso ao prédio temporária ou permanentemente)**

- Manuenção: pedreiros, pintores, eletricistas, técnicos em telefonia, hardware, redes, internet, etc,  
 - Zeladores, chefes, diretores, etc  
 - Programadores, técnicos em segurança, analistas, DBA, etc  
 - etc

### **Estrutura física**

- Prédio  
 - Instalações elétricas, fios, estabilizadores, no-breaks, etc  
 - Instalações de ar condicionado,  
 - Instalações telefônicas,  
 - Dispositivos contra incêndios,  
 - Instalações de rede: cabos, conectores, switches, etc  
 - Estrutura de internet: cabos, placas, roteadores, etc  
 - Hardware: firewalls, computadores, storages, etc  
 - etc

### **Permissões de arquivos e diretórios**

As permissões de arquivos e diretórios no Linux costumam ser um tópico confuso que leva a diferentes visões, especialmente no caso de diretórios e arquivos da web. O pior conselho, que nunca deve ser seguido, é alterar arquivos ou pastas para 777. Isso permite que qualquer pessoa no mundo execute ou grave em seu servidor. O melhor exemplo disso são os plug-ins nocivos do WordPress que hackers mal-intencionados enviam aos servidores por meio de um simples comando HTTP POST. Se as permissões de diretório forem 777, isso permite que qualquer pessoa leia, escreva ou execute qualquer coisa nesse diretório, incluindo a publicação de código malicioso.  
Muitos usuários do WordPress em particular foram recentemente comprometidos por um plugin malicioso que foi instalado porque os usuários incorporaram 777 permissões na instalação do WordPress.  
  
Em geral, os diretórios devem ser 750 ou 755. Os arquivos devem ser 644 ou 640.  
  
Localize os diretórios com 777 em seu servidor:  
  
sudo find /var/www/ -type d -perm -002  
  
Localize os arquivos com 777 em seu servidor:  
  
sudo find /var/www/ -type f -perm -002  
  
Além das permissões também precisamos ficar atentos para os donos dos arquivos/diretórios.  
  
**Aplicativos PHP**  
  
A execução de PHP em um servidor Linux é necessária para muitos aplicativos populares, como Drupal, WordPress e outros. Novas vulnerabilidades são encontradas não apenas no código PHP mal escrito, mas na própria linguagem em uma taxa alarmante. Visto que o PHP costuma ser emparelhado com o MySQL, um comprometimento do PHP pode significar um comprometimento do banco de dados MySQL que o acompanha para o servidor web. Para esses fins, é essencial estar atento a qualquer software PHP ou atualizações de plug-in. Não instale ou use código PHP de fontes desconhecidas. Para software de blog, minimize o número de plug-ins ou extensões em uso. Se um plug-in ou complemento não estiver ativado ou em uso para o blog ou site, remova os arquivos não utilizados do servidor.  
  
Certifique-se de que as páginas 404 para o servidor não forneçam informações estranhas e não interpretem o que foi colocado na barra de URL. Visite uma página 404 aleatória no servidor da web como um teste, como http://example.com/asdf. Os resultados da página 404 devem fornecer apenas um "Desculpe, essa página não foi encontrada" genérica e não tentar interpretar ou retransmitir os resultados que o usuário colocou na barra de URL. As páginas 404 que permitem a manipulação da entrada do usuário são um ponto de entrada para invasores criarem XSS e outras tentativas maliciosas.

### **Recomendações sobre Segurança**

Os cuidados com a segurança colaboram para que os sites e aplicativos instalados no servidor sejam executados de forma esperada, rápida e sem interrumpção.  
  
- Hospede seu site em servidor seguro  
- Efetue backup regularmente, especialmente a cada alteração no site  
 A melhor opção atualmente para backup é o Akeeba Backup - https://www.akeebabackup.com/download.html  
 Caso tenha dificuldade de usar o formato JPA, altere em Configuration - Archiver engine para ZIP format  
 Ele gera o backup com um instalador. Para restaurar apensa instale como se fosse instalar o Joomla  
 Faça também backup dos scripts de configuração do servidor para o caso de uma reinstalação  
 Lembre de fazer o backup do servidor com os recursos da hospedagem ou crie um snapshot  
- Também faça teste de restore de vez em quando para garantir que o backup está integro, usando o kickstart  
- A quantidade de cópias de backup a ser guardada depende da importância do site. Se mais importante mais cópias  
- As cópias devem ser armazenadas em mídia confiável: HD e DVD  
- Efetue atualização com frequência. Mantenha o aviso de atualização ativo para que receba um aviso por e-mail e atualize imediatamente  
- Após a primeira atualização reinicie o servidor  
- Acessar de forma segura usando SSH (enxuto e configurado para salvar a senha) e nunca via FTP  
- Manter seu desktop seguro, usando um sistema operacional seguro no mesmo, com firewall e outros cuidados  
- Use e abuse da comunidade com seus conhecimentos e generosidade para manter-se atualizado em termos de segurança e proteger seu site  
- Use senhas fortes  
- Use o SSL para proteger pelo menos o administrator  
- Use boas extensões para reforçar a segurança  
- Remova todas as extensões que não estiver usando e não somente desabilite  
- Evite instalar pacotes para desenvolvimento como gcc, make, etc e evite também instalar repositórios instáveis.  
- Monitorar frequentemente os logs à procura de algo suspeito em todos os serviços ativos  
- Use softwares tipo IDS que detectam intrusões  
- Instalar um bom firewall de aplicativos como o mod\_security  
- Ficar bem atento, estudando, se informando sempre sobre o assunto de que cuida  
- Logo após a configuração final do servidor já crie um backup ou snapshot da droplet e fique atento para criar outro logo que o servidor esteja concluído e bem configurado.  
- Uma boa ideia é ter no desktop a mesma distro e versão do Linux. Para quem usa Windows uma box no Vagrant do Ubuntu 20.04 em seu desktop, sendo cópia fiel e original do servidor localmente, mesma distribuição, mesma versão  
- E use algumas ferramentas que reforçam a segurança como:  
fail2ban  
denyhosts  
lynis  
rhhunter  
etc  
  
- Usar senhas de no mínimo 8 caracteres. Quanto mais melhor  
- Misturar caracteres alfabéticos maiúsculas, minúsculas, números e caracteres especiais como:  
-, \_, \*, $, !, %  
- Não use senhas fáceis como data de nascimento, número de identidade, nomes de filhos e cônjuges.  
- Procure não usar palavras do mundo real  
- Pense num eposódio que apenas você conhece ou lembra e forme uma frase com suas iniciais  
- Crie senhas posicionais, por exemplo: primeira letra da última fila, primeira letra da primeira fila, última letra da última fila, última letra da primeira fila e assim por diante.  
- Mesmo que ilógicas as senhas devem ser, para você, de fácil memorização, pois você deve evitar anotar as senhas  
- Evite usar a mesma senha para todos os esus acessos  
- Atualize com uma certa frequeência suas senhas  
  
  
Evitar o uso do ftp para transferir/baixar arquivos para/do servidor, pois ele envia seus dados (login e senha) em texto claro.  
  
Se precisar usar o ftp use o FileZilla, que usa o sftp.  
  
https://filezilla-project.org/

### **Uma forte política de segurança nas senhas**

**Então, quais são as "melhores práticas" ao configurar senhas?**  
 1. Use senhas tão longas quanto você possa gerenciar  
 2. Evite palavras que aparecem no dicionário (como "uvas azuis")  
 3. Evite substituições de números que sejam fáceis de adivinhar (como "h3ll0")  
 4. Não faça referência à cultura pop (como “TARDIS”)  
 5. Nunca use uma senha em mais de um lugar  
 6. Altere sua senha regularmente e use uma diferente para cada site  
 7. Não anote as senhas e não as compartilhe. Não com ninguém. Sempre!  
   
**Bloqueando contas de usuário após logins malsucedidos**  
  
Para a segurança do Linux, o comando faillog mostra tentativas de login malsucedidas e pode atribuir limites para quantas vezes um usuário pode obter suas credenciais de login erradas antes que a conta seja bloqueada. faillog formata o conteúdo do log de falha do banco de dados de log  
/var/log/faillog. Para visualizar as tentativas de login malsucedidas, digite:  
  
faillog  
  
**Para abrir uma conta bloqueada desta forma, execute:**  
  
faillog -r -u userName  
  
Com a segurança do Linux em mente, você pode usar o comando passwd para bloquear e desbloquear contas:  
  
**Bloquear uma conta**  
  
passwd -l userName  
  
**Desbloquear**  
  
passwd -u userName

### **Sites com Gerenciador de Conteúdo**

Analisando os fatores abaixo em sites para gerenciamento de conteúdo.  
  
**Segurança, performance, custo e usabilidade**  
  
Estes são quatro entre os fatores mais importantes para sites. Vou aqui analisar algumas das alternativas que já experimentei para a criação e gerenciamento de sites de conteúdo ou blogs.  
  
**Tipos de sites:**  
  
- Site estático, somente HTML, CSS e pouco Javascript. Na maioria usando Bootstrap.  
- Usando um CMS  
  
Segurança - a melhor alternativa que já experimentei em termos de segurança é usando site estático, visto que não usa servidores como Apache ou MySQL nem linguagem dinâmica e outros fatores próprios dos sites criados com CMS, geralmente com Apache, MySQL e PHP. Um princípio da segurança: quanto menos recursos usar mais seguro.  
  
Performance - a melhor performance que conheço é um site com apenas HTML, sem CSS ou JS. Mas não fica um site bonito, nem fica responsivo, que é um tipo de site atualmente de grande importância, pois se adapta automaticamente para as dimensões do dispositivo que acessa o site. Como atualmente temos uma grande quantidade de pessoas acessando internet com dispositivos móveis, talvez a maioria, então um site com apenas HTML é praticamente inviável. A forma mais pratica que conheço e tenho usado é pegar um template bonito, geralmente com o Bootstrap e adaptado. Aqui precisamos tomar cuidado, em termos de performance, com o Javascript, que pode degradar a eprformance. Jś um site criado com um CMS tem todo as consequências do uso de servidores, que o torna menos performático. Também temos CMS que geram sites estáticos e softwares que geram sites de documentação, com certa praticidade, mas vejamos os demais fatores.  
  
Custo - Este é o terceiro fator em que os sites em HTML estáticos são vencedores. Existem boas hospedagens free para sites estáticos. A minha melhor esperiência é com o Github, que inclusive suporta nosso domínio por lá. Praticamente não existe um bom servidor de hospedagem free para CMS. Existem alguns poucos que podemos usar, mas apenas para testes e não para um site em produção.  
  
Usabilidade - Este fator precismos dividir em duas áreas: usabilidade para o visitante e usabilidade para quem cria e administra o site e especialmente o conteúdo. Em termos de visitante um site estático pode sem grande dificuldade para quem cria, melhor para quem adapta um template, pode deixar a usabilidade para o visitante bem suave. Praticamente nada perde para a usabilidade de um site criado com um CMS.  
  
Até aqui os sites estáticos ou ganharam dos sites criados com CMS ou empataram. Mas agora vamos analisar a usabilidade para quem cria, gerencia o site e/ou gerencia o conteúdo. Este é o ponto forte dos sites criados com CMS, especialmente no gerenciamento do conteúdo, que praticamente é feito num editor HTML amigável, parecido com um bom processador de textos, como o Word ou o do LibreOffice.  
  
Veja que não é simplesmente contar em quantos fatores um tipo de site leva vantagem, pois os do tipo de sites estáticos levam vantagem em 3 dos 4 fatores e empatam em parte do quarto, mas perdem apenas na última parte do quarto fator e esta parte é vital para a maioria dos sites com gerenciamento de conteúdo.  
  
Algo que é inviável é criar um site estático e entregar para um cliente leigo alimentar o conteúdo. Talvez se possa ministrar um treinamento para ele mas não vou considerar isso como viável. Ele precisará entender de HTML, CSS e JS, qua praticamente nenhum cliente que conheço sabe.  
  
Algo importante é o carregamento de páginas usando JS ou AJAX. No jQuery existe um método de AJAX chamado 'load', que carrega um uma página outras páginas, tipo um include do PHP. Acontece que é'algo complexo de fazer para que fique algo decente. Vejo vários sites, mesmo de grandes empresas, que usam este recurso mas de forma feia. A página carrega primeiro sem o CSS e em seguida carrega com o CSS. Imagino que estejam usando um site estático por conta da segurança e não se preocupam com isso do load, nem tem alguém fiscalizando que entenda e exiga algo decente. Sei que isso é apenas estético, mas dá para fazer melhor.

### **Segurança no Joomla (parte 1)**

Dicas de segurança no joomla.  
Muitas pessoas utilizam o CMS Joomla, no entanto a maior parte destas "esquece-se" do fator segurança nos seus sites. Existem pequenos pormenores extremamente fáceis de implementar que aumentarão consideravelmente a segurança do teu site Joomla.  
  
**Desligar os relatórios de erro**  
  
Um deles é desligar os relatórios de erros, os relatórios de erros alem de diminuírem a velocidade do site indicarão também ao "hackers" falhas na segurança deste. Isto pode ser desativado em 'Configuração Geral -> Sistema'.  
  
Depois de desativada esta função não te será permitido visualizar os erros gerados pelo Joomla, o que é uma coisa boa uma vez que o utilizador comum não os vê (o que não era muito profissional) e os hackers não podem forçar erros de forma a descobrirem métodos de comprometer o sistema.  
  
**Utilizar um componente SEF**  
  
A maioria dos hackers utilizam o comando 'inurl:' do Google para procurarem por falhas em websites. Uma boa solução para contrariar este potencial risco é instalar um componente que re-escreva os Url, aconselho o SH404SEF ou o Artio-JoomSef.  
  
O componente SEF irá trazer-lhe também bastantes vantagens a nível de SEO (rank mais elevado aos "olhos" do Google).  
  
  
Mover o ficheiro configuration.php para fora da raiz.  
Mova simplesmente o ficheiro de configuração para qualquer pasta que você queira dentro do site e atribua-lhe um novo nome. No exemplo utilizei 'joom.conf'.  
Crie um novo ficheiro de configuração na raiz com o nome de configuration.php contendo o seguinte código:

<?php  
require( dirname( \_\_FILE\_\_ ) . '/../joom.conf' );  
?>  
  
**Realize backups regulares**  
  
Esta tarefa pode ser feita através do Cpanel de qualquer conta de alojamento, no entanto existem também alguns componente muito bons que realizam esta tarefa. O meu favorito é o JoomlaPack. Um backup semanal caso atualize o seu site regularmente é uma boa opção, ou então backups mensais.  
  
  
**Não mostrar que versões das extensões utiliza**  
  
Em primeiro lugar qualquer admin de um website deveria ter uma lista de todas as extensões que utiliza e fazer o update a estas quando sai-se uma nova versão. No entanto todos nos sabemos que o tempo não chega para tudo e muitas vezes fazer um update a uma extensão pode ser um bocado moroso. É então boa política remover a versão da extensão que utiliza a quando da instalação desta, isto pode ser feito editando os ficheiros da extensão com o notepad por exemplo.  
  
  
**Segunda parte**  
  
Um site em Joomla! é muito mais do que instalá-lo no servidor, mover alguns módulos de posição, instalar componentes, plugins e pronto! Já temos um site completo, feito em três dias e podemos ganhar mais de mil reais do nosso cliente.  
  
Sinceramente, pessoal, o Joomla é tão complicado de usar quanto se programar um site do zero. Claro que você não terá mais a necessidade de digitar todas as linhas de código, mas eventuais alterações serão necessárias e é importante saber o que, onde e por que está sendo feita aquela mudança.  
  
Além disso, a segurança é muito importante. Hoje existe uma gama enorme de componentes e módulos para Joomla, mas antes de usarem, perguntem-se: "este componente é seguro?". A maioria das invasões em sites Joomla! é feita através do próprio cms mal configurado ou de seus componentes desatualizados. Experiência própria: é muito mais difícil você contornar uma invasão do que prevenir que ela não aconteça.  
  
Trabalho com o Joomla há mais de três anos, desde a versão 1.0.12, e desde lá já aprendi muito, tomei muito na cabeça e hoje me viro tranqüilo, tanto é que tenho mais de 20 clientes em minha região e todos utilizam o Joomla!, mas a cada nova atualização de componentes, preciso dar atenção a estes sites, pois é a segurança dos dados e informações dos mesmos que estão em jogo.  
  
Por isso minha gente, tenho um sério conselho a dar a vocês: Estudem!  
  
Estudem muito o Joomla, pesquisem sobre servidores web (apache), sobre dicas de segurança no PHP, informações sobre servidores de e-mail, segurança de arquivo, permissões de acesso a pastas e arquivos, etc...  
  
Mostrei apenas o caminho das pedras, agora é Google na veia e tempo e disciplina para estudar. Hoje existem mil vezes mais materiais sobre esse assunto do que quando comecei. Inclusive a maioria mais detalhada e em português, no "meu tempo" os bons artigos e tutoriais eram em inglês.  
  
Este e-mail foi escrito como um alerta aos desavisados, para não saírem por ai usando o Joomla! sem considerar o uso de medidas sobre segurança.  
  
Isso evitará os seus sites de serem invadidos e assim o indivíduo não vai sair por ai xingando todo mundo em qualquer fórum destinado ao Joomla!, falando mal do sistema para qualquer um que aparecer, alegando que "não é seguro".  
  
Quem faz o Joomla ser seguro é você".  
Escrito por Roberto Jonikaites para o Yahoogrupos – Curso de Design para Joomla! De Bruno Ávila.  
  
Este artigo foi encontrado no sitea baixo, mas faz um bom tempo que este domínio não está ativo, nem mesmo o raiz (http://www.joomlarj.com.br). Outra providência que uso nestas casos é efetuar uma pesquisa pelo título, já que o domínio está fora, assim, usando aspas duplas cercando o título, para que o Google mostre somente sites que contiverem exatamente a frase:  
  
**"Segurança no Joomla (parte 1)"**  
  
**Olha o que o Google ke diz:**  
  
Nenhum resultado encontrado para "Segurança no Joomla (parte 1)".  
  
Ou seja, o autor publicou apenas no domínio joomlarj.com.br. Ainda bem que guardei e estou divulgando aqui. Caso ele reclame será removido sem problema.  
  
<http://www.joomlarj.com.br/site/index.php?option=com_content&view=article&id=26:seguranca-no-joomla-parte-2&catid=15:seguranca-no-joomla&Itemid=15>  
  
Windows 64  
<https://filezilla-project.org/download.php?platform=win64>

Referências  
  
<https://geek.linuxman.pro.br/geek/ubuntu-pronto-para-guerra>  
<https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics>  
<https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/>  
<https://hostpresto.com/community/tutorials/how-to-install-and-use-lynis-on-ubuntu-14-04/>

### **Monitorando o servidor**

Monitorando o servidor com recursos do painel administrativo do DigitalOcean  
  
O Digital Ocean tem em seu painel administrativo, uns gráficos de uso dos recursos:  
- Consumo de banda, Uso da CPU e leitura e escrita de disco (I/O)  
- Acessar o painel efetuando login  
- Selecionar a droplet desejada  
Aparecerá o gráfico ao centro.  
  
Bandwidth - clique abaixo em private inbound para ver o seu uso e em public inbound para ver o uso externo  
CPU Usage - clique em sys para ver o consumo pelo sistema e em user para ver o consumo do usuário  
Disk I/O - clique em read para ver o uso de leitura e em write para ver o de escrita.  
(Existem outros recursos caso se faça upgrade da droplet)  
  
Acima e à direita exite uma combo que mostra por default Last 1 hour (Gráfico da última hora). Podemos mudar para quue mostre mais horas e até dias. Colado à direita tem outra combo com 5m, que é o tempo de refresh do gráfico, que podemos alterar.  
  
Se passarmos o ponteiro do mouse sobre o gráfico podemos ver detalhes pontuais.  
  
https://www.digitalocean.com/docs/droplets/how-to/graphs/  
  
Configurando monitores de alerta da droplet  
  
https://www.digitalocean.com/docs/monitoring/how-to/set-up-alerts/  
  
O Monitoramento DigitalOcean é um serviço opcional gratuito que reúne métricas sobre a utilização de recursos no nível do Droplet. Ele fornece gráficos Droplet adicionais e oferece suporte a políticas de alerta de métricas configuráveis com notificações Slack por e-mail integradas para ajudá-lo a rastrear a integridade operacional de sua infraestrutura.  
  
Este é um recurso que emite um alerta quando algum recurso atinge certo consumo. Para criar um Alert:  
  
- Selecione a droplet  
- à esquerda clique em Manage - Monitoring - Create Aelrt Policy  
- Clique em CPU para escolher o tipo de Alert (CPU, Banda entrada, saída, Disco leitura, escrita, Memória, Utilização de disco).  
 CPU  
 is above/acima  
 70%  
 5 min  
   
 Role a tela e entre com o nome da droplet ou uma tag  
 Send alerts via e-mail  
 Name - CPU com consumo elevado  
 Create alert policy  
   
 Significa: Quando o uso da CPU estiver acima de 70% por 5 minutos me avise.  
  
  
**Monitorar os recursos**  
  
Espaço em disco  
  
df -h  
Memória RAM e Swap  
  
free -m  
  
  
Sites com serviço online de monitoramento, com plano free  
  
- <https://www.statuscake.com/>  
  
Uptime Monitoring Server Monitoring  
Domain Monitoring Page Speed Monitoring  
SSL Monitoring Virus Scanning

### **Monitoramento dos Logs**

Os logs são uma parte crítica para monitorar a segurança de um servidor web. Existem muitas ferramentas em distribuições Linux para automatizar o monitoramento de log. O aplicativo logwatch envia um relatório diário de e-mail de todos os logs no servidor para informar sobre entradas de log variáveis, como o número de e-mails enviados, invasores da web em potencial e IPs causando erros nos logs do Apache, tentativas de ssh e outros aspectos.  
  
Em um grande ambiente corporativo, é comum enviar emails logwatch junto com outros emails direcionados ao usuário root (erros de cron e outras mensagens do sistema) para uma única lista de emails da empresa. Os administradores da empresa, então, se inscrevem nessa única lista de e-mail para se manterem informados sobre quaisquer notificações alarmantes nos registros de vários servidores da empresa.  
  
<https://resources.infosecinstitute.com/topic/securing-linux-web-server/>

### **PHP**

**PHP configurations to be made in php.ini:**  
[sourcecode]  
expose\_php = Off  
display\_errors = Off  
track\_errors = Off  
html\_errors = Off  
  
**Após configurar repita**  
  
curl -I example.com

### **Apache**

**Vazamento de informação**  
As primeiras mudanças de configuração relativamente triviais que devem ser feitas são para desabilitar qualquer vazamento de informações de seu servidor. Todas as distribuições do Linux têm configurações padrão pobres em relação ao vazamento de informações para o Apache e outros serviços. Embora a maioria descarte isso como não sendo uma preocupação, quanto menos informações você transmitir para um hacker, melhor. Cada solicitação ao servidor da web Apache pode responder com informações, como a versão exata do OpenSSL, versão do PHP e muitos outros itens.

Embora alguns aplicativos como o OpenSSH exijam a transmissão de sua versão no banner para operação, não há razão funcional para o Apache transmitir seu número de versão para o mundo, e da mesma forma, nem qualquer outro módulo Apache relacionado.

Buscar os cabeçalhos HTTP com curl como exemplo pode fornecer as seguintes informações publicamente:  
  
curl -I example.com  
  
**Apache configurations:**  
  
ServerTokens Prod  
ServerSignature Off  
TraceEnable Off  
Header unset ETag  
FileETag None